#4

Docket No. 21.1958/MS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Hideto YASUDA et al.

Serial No.: NEW

Filed: April 4, 2000

Group Art Unit:

Examiner:

For: USER AUTHENTICATION APPARATUS, METHOD OF USER AUTHENTICATION, AND STORAGE MEDIUM THEREFOR

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. §1.55

Honorable Commissioner of Patents and Trademarks
Washington, D.C. 2023l

Sir:

In accordance with the provisions of 37 C.F.R. §1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application:

Japanese Patent Application No. 11-198061
Filed: July 12, 1999

It is respectfully requested that the applicants be given the benefit of the foreign filing date as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. §119.

Respectfully submitted,

STAAS & HALSEY LLP

By: _____
J. Randall Beckers
Registration No. 30,358

700 11th Street, N.W., Ste. 500
Washington, D.C. 20001
(202) 434-1500

Date: 4/4/2000

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９９年 ７月１２日

出 願 番 号
Application Number: 平成１１年特許願第１９８０６１号

出 願 人
Applicant (s): 富士通株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

１９９９年 ８月２６日

特 許 庁 長 官
Commissioner,
Patent Office 伊佐山建志

【書類名】　特許願

【整理番号】　9950479

【提出日】　平成11年 7月12日

【あて先】　特許庁長官殿

【国際特許分類】　G06F 15/00

【発明の名称】　認証制御装置、認証制御システムおよび認証制御方法並びに記録媒体

【請求項の数】　10

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　安田　英人

【発明者】

【住所又は居所】　長野県松本市深志１丁目１番１５号　株式会社富士通パソコンラボ内

【氏名】　大澤　智人

【特許出願人】

【識別番号】　000005223

【氏名又は名称】　富士通株式会社

【代理人】

【識別番号】　100072590

【弁理士】

【氏名又は名称】　井桁　貞一

【電話番号】　044-754-3035

【手数料の表示】

【予納台帳番号】　011280

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9704486

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　認証制御装置、認証制御システムおよび認証制御方法並びに記録媒体

【特許請求の範囲】

【請求項１】　利用者により入力される入力識別情報と記録媒体に記録されている固有の識別情報との照合を制御する制御部と、

前記照合結果に応じて、前記記録媒体に記録されている複数のシステムにそれぞれ対応する認証情報のうち読み出される対象システムに関する認証情報を認証処理の入力情報として設定する設定部と、

を備える認証制御装置。

【請求項２】　利用者により入力される入力識別情報と記録媒体に記録されている固有の識別情報との照合を制御する制御部と、

前記照合結果に応じて、前記記録媒体に記録されている対象システムに関する認証情報を利用者により入力された新たな認証情報への変更を制御する変更制御部と、

前記記録媒体に記録された認証情報の変更に同期して、前記入力された新たな認証情報を用いてシステムが保持している認証情報を変更する変更処理部と、

を備える認証制御装置。

【請求項３】　利用者により入力される入力識別情報と記録媒体に記録されている固有の識別情報との照合を制御する制御部と、

前記照合結果に応じて、前記記録媒体に記録されている複数の証明書の中から所望の証明所の読み出しを指示する指示部と、

前記記録媒体から読み出される前記指示された証明書をシステムに供給する供給部と、

を備える認証制御装置。

【請求項４】　複数のシステムにそれぞれ対応する認証情報と固有の識別情報とを保持する記録媒体と、前記記録媒体に保持されている認証情報をシステムでの認証に用いる装置からなる認証制御システムであり、

前記装置は、

利用者により入力される入力識別情報と記録媒体に記録されている固有の識別情報との照合を制御する制御部と、

前記照合結果に応じて、前記記録媒体に記録されている複数のシステムにそれぞれ対応する認証情報のうち読み出される対象システムに関する認証情報を認証処理の入力情報として設定する設定部とからなる、

認証制御システム。

【請求項５】　複数のシステムにそれぞれ対応する認証情報と固有の識別情報とを保持する記録媒体と、前記記録媒体に保持されている認証情報をシステムでの認証に用いる装置からなる認証制御システムであり、

前記装置は、

利用者により入力される入力識別情報と記録媒体に記録されている固有の識別情報との照合を制御する制御部と、

前記照合結果に応じて、前記記録媒体に記録されている対象システムに関する認証情報を利用者により入力された新たな認証情報への変更を制御する変更制御部と、

前記記録媒体に記録された認証情報の変更に同期して、前記入力された新たな認証情報を用いてシステムが保持している認証情報を変更する変更処理部とからなる、

認証制御システム。

【請求項６】　利用者により入力される入力識別情報と記録媒体に記録されている固有の識別情報とを照合し、

前記照合結果に応じて、前記記録媒体に記録されている複数のシステムにそれぞれ対応する認証情報のうち対象システムに関する認証情報を読み出し、

前記読み出された認証情報を認証処理の入力情報として設定する、

認証制御方法。

【請求項７】　利用者により入力される入力識別情報と記録媒体に記録されている固有の識別情報との照合し、

前記照合結果に応じて、前記記録媒体に記録されている対象システムに関する認証情報を利用者により入力された新たな認証情報へ変更し、

前記記録媒体に記録された認証情報の変更に同期して、前記入力された新たな認証情報を用いてシステムが保持している認証情報を変更する、

認証制御方法。

【請求項８】　認証処理に用いられる認証情報を記録する記録媒体であって、

外部と情報を授受する送受信部と、

システムを特定するシステム識別情報と該システム識別情報に対応付けられた認証情報との組を複数記録すると共に媒体固有の情報を記録する記録部と、

外部から供給される情報と前記固有情報の照合を行う照合部と、

前記照合結果に応じて前記認証情報を外部に供給する処理部と、

を備える記録媒体。

【請求項９】　コンピュータに、

利用者により入力される入力識別情報と記録媒体に記録されている固有の識別情報との照合を制御する手順と、

前記照合結果に応じて、前記記録媒体に記録されている複数のシステムにそれぞれ対応する認証情報のうち読み出される対象システムに関する認証情報を認証処理の入力情報として設定する手順と、

を実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項１０】　コンピュータに、

利用者により入力される入力識別情報と記録媒体に記録されている固有の識別情報との照合を制御する手順と、

前記照合結果に応じて、前記記録媒体に記録されている対象システムに関する認証情報を利用者により入力された新たな認証情報への変更を制御する手順と、

前記記録媒体に記録された認証情報の変更に同期して、前記入力された新たな認証情報を用いてシステムが保持している認証情報を変更する手順と、

を実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、装置やシステム、サービスなどの利用を許可するために行われる利用者認証に関するものである。

【０００２】

近年、ネットワークの整備やパーソナルコンピュータ、通信装置などのハードウェアが安価になったことから、家庭や企業内さらには屋外などの様々な場所において誰でもインターネットを利用した電子メールの送受信やＷＷＷ（Ｗｏｒｌｄ　Ｗｉｄｅ　Ｗｅｂ）閲覧などが簡単にできるような環境になってきている。

【０００３】

また、企業においては、イントラネットやエクストラネットにより業務の迅速化、効率化を図っており、従来のメインフレームを中心としたホスト集中型の業務システムに加え、ネットワークを利用してクライアント／サーバ型の業務システムを構築し、運用を行っている。

【０００４】

上述のように、家庭や企業において様々なシステムを誰でも利用することが可能となっているが、このようなシステムやサービスにおいては、これらを利用する際に利用者固有のＩＤとパスワードを入力させ、その入力情報を使用して利用資格があるか否かを判断する認証処理が通常行われている。

【０００５】

さらに、パーソナルコンピュータのオペレーティングシステムにおいても、利用者を制限するためや利用者に応じて各種環境設定を変えるために、ＩＤとパスワードを用いた認証処理が適用されるようになっている。

【０００６】

【従来の技術】

このように、家庭や屋外、企業内において様々なシステムやサービス（以下、総称してシステムとする）を利用するために、利用者は各システムに対応するＩＤとパスワードの組を複数記憶しておく必要がある。

【０００７】

利用するシステムの数が少なければ利用者はＩＤとパスワードを記憶しておくことが可能であるが、複数のシステムを利用する利用者はシステムの数が多くなればＩＤとパスワードを忘却してしまうという事態に陥ってしまう。

【０００８】

このＩＤとパスワードを忘却することでシステムを利用できなくなるという状況を避けるため、利用者の多くは手帳などに各システム毎のＩＤとパスワードをメモし、認証処理の際に手帳を見て得られるＩＤとパスワードを入力するというシステムの利用形態をとっているのが一般的である。

【０００９】

また、企業内においては、従業員番号情報を記録した磁気カードを従業員に配布し、その磁気カードを使用して認証処理を行うというシステムの運用形態をとることも行われている。

【００１０】

他の従来技術として、信頼度を強化し、必要十分な認証を可能とする特開平７－６４９１１号がある。

【００１１】

この公開公報においては、１つのホストコンピュータとそれに接続される複数の端末で構成されるシステムにおいて、ＩＣカードや磁気カードに複数の個人認証データ（識別情報、パスワード、筆跡、指紋など）を記憶させておき、端末には複数の個人認証データを入力できるよう、キーボードやタブレット、磁気カード読取部、ＩＣカード読取部を備え、それらの内のいくつかを選択して複数の個人認証データを入力し、照合することが開示されている。

【００１２】

【発明が解決しようとする課題】

上述のように、認証処理の際に、手帳にメモしたＩＤとパスワードを見て入力するという利用形態においては、手帳の内容を他人に見られＩＤとパスワードが漏れてしまい、システムが不正利用されるという問題が発生している。

【００１３】

また、磁気カードを用いる認証処理は磁気カードを読取装置で読ませるだけと

いう利用者による操作が簡易であるという利点があるが、本来の所有者以外の他人が磁気カードを読取装置に読ませることだけで認証が行われてしまい、セキュリティが脆弱でシステムへの不正アクセスを防止できない。

【００１４】

さらに、特開平７－６４９１１号においては、複数の個人認証データを使用するということでセキュリティの効果は大きいが、１つのシステムに対するセキュリティは向上できるものの複数のシステムに対するセキュリティの向上、利用者による認証操作の簡易化は想定されているものではない。

【００１５】

本発明は、複数のシステムに対する利用者の操作の簡易化、複数のシステムを利用する環境におけるセキュリティ向上のための認証制御装置、認証制御システム、記録媒体を提供することを目的とする。

【００１６】

【課題を解決するための手段】

上記目的を達成するために、本発明では、利用者により入力される入力識別情報と記録媒体に記録されている固有の識別情報との照合を制御する制御部と、前記照合結果に応じて、前記記録媒体に記録されている複数のシステムにそれぞれ対応する認証情報のうち読み出される対象システムに関する認証情報を認証処理の入力情報として設定する設定部とで装置を構成する。

【００１７】

また、利用者により入力される入力識別情報と記録媒体に記録されている固有の識別情報との照合を制御する制御部と、前記照合結果に応じて、前記記録媒体に記録されている対象システムに関する認証情報を利用者により入力された新たな認証情報への変更を制御する変更制御部と、前記記録媒体に記録された認証情報の変更に同期して、前記入力された新たな認証情報を用いてシステムが保持している認証情報を変更する変更処理部とで装置を構成する。

【００１８】

また、利用者により入力される入力識別情報と記録媒体に記録されている固有の識別情報との照合を制御する制御部と、前記照合結果に応じて、前記記録媒体

に記録されている複数の証明書の中から所望の証明所の読み出しを指示する指示部と、前記記録媒体から読み出される前記指示された証明書をシステムに供給する供給部とで装置を構成する。

【００１９】

また、本発明の特徴を備えた上記装置と上記記録媒体からなるシステムとして構成してもよい。

【００２０】

また、上記記録媒体を、外部と情報を授受する送受信部と、システムを特定するシステム識別情報と該システム識別情報に対応付けられた認証情報との組を複数記録すると共に媒体固有の情報を記録する記録部と、外部から供給される情報と前記固有情報の照合を行う照合部と、前記照合結果に応じて前記認証情報を外部に供給する処理部とで構成する。

【００２１】

さらに、コンピュータである装置を制御するプログラムを、利用者により入力される入力識別情報と記録媒体に記録されている固有の識別情報との照合を制御する手順と、前記照合結果に応じて、前記記録媒体に記録されている複数のシステムにそれぞれ対応する認証情報のうち読み出される対象システムに関する認証情報を認証処理の入力情報として設定する手順とを実行させるよう構成する。

【００２２】

また、コンピュータである装置を制御するプログラムを、利用者により入力される入力識別情報と記録媒体に記録されている固有の識別情報との照合を制御する手順と、前記照合結果に応じて、前記記録媒体に記録されている対象システムに関する認証情報を利用者により入力された新たな認証情報への変更を制御する手順と、前記記録媒体に記録された認証情報の変更に同期して、前記入力された新たな認証情報を用いてシステムが保持している認証情報を変更する手順とを実行させるよう構成する。

【００２３】

【発明の実施の形態】

以下、本発明の実施の形態について説明する。

【００２４】

本発明の実施形態においては、ネットワークを介して接続されるクライアント／サーバシステムを例として説明する。なお、本例のようにクライアント／サーバシステムではなく、メインフレームを中心としたホスト集中型のシステムであっても構わない。

【００２５】

図１は、本発明のシステム構成図である。

【００２６】

図１に示されるように、クライアント１はネットワーク３を介してサーバ２に接続される。そして、クライアント１はサーバ２にアクセスし、サーバ２上のアプリケーションソフトを利用した業務処理や、サーバ２からデータのダウンロード処理などを行う。

【００２７】

図２は、クライアント１であるコンピュータの概略構成を示す図である。

【００２８】

クライアント１は、主に、ＣＰＵ４，ＲＡＭ５，ＨＤＤ（ハードディスクドライブ）６，ＣＤ－ＲＯＭドライブ７，ＦＤＤ（フロッピィディスクドライブ）８，ＮＣＵ（ネットワーク制御ユニット）９，ディスプレイ１０，キーボード１１，ＩＣカードリーダライタ１２から構成される。

【００２９】

図中、ＣＰＵ４はプログラムにより各種処理、制御を実行するものであり、本発明のプログラムによる各種処理、制御においても使用される。

【００３０】

また、ＲＡＭ５はＣＰＵ４による各種処理や制御のための一時的なデータの保持や、ディスプレイ１０に表示するためのデータを保持するために使用される。

【００３１】

ハードディスクドライブ６およびフロッピィディスクドライブ８は、プログラムや制御データを不揮発性の記録媒体（ハードディスクやフロッピィディスク１４）に記録したり、該記録媒体からプログラムや制御データを読み出すためのデ

バイスである。

【００３２】

ＣＤ－ＲＯＭドライブ７はＣＤ－ＲＯＭ１３に記録されたプログラムや制御データを読み出すためのデバイスである。

【００３３】

ネットワーク制御ユニット９は、ネットワーク３に接続し、ネットワーク３を介して他の装置とのデータのやり取りを行うものである。このネットワーク制御ユニット９によりネットワーク３を介してサーバ２とのデータの授受が可能となる。

【００３４】

このネットワーク制御ユニットは、モデムであってもいいし、ＬＡＮカードであってもよい。

また、サーバ２からのプログラム、データのダウンロードやサーバ２が提供するサービスを受けるためにも使用できる。

【００３５】

クライアント１で動作する本発明のプログラムはＣＤ－ＲＯＭ１３やフロッピィディスク１４などに記録されているものをそれぞれＣＤ－ＲＯＭドライブ７やフロッピィディスクドライブ８などによって読み取り、ハードディスクドライブ６の記録媒体にインストールされるものである。

【００３６】

また、上記本発明のプログラムをネットワーク制御ユニット９によりネットワークを介して他の装置からダウンロードしてハードディスクドライブ６の記録媒体に格納するようにしてもよい。

【００３７】

このようにしてハードディスクドライブ６の記録媒体に格納された本発明のプログラムは、実行指示によりＲＡＭ５にロードされ、ＣＰＵ４を制御して本発明の各構成要件をコンピュータであるクライアントにて実現するよう動作する。

【００３８】

上記のように、本発明のプログラムを一旦ハードディスクドライブ６の記録媒

体に格納するという形態ではなく、ネットワークを介して他の装置からダウンロードしてＲＡＭ５に直接展開するよう構成してもよい。

【００３９】

ディスプレイ１０はＲＡＭ５に保持されるデータを画面上に表示するためのものである。

【００４０】

キーボード１１は主にユーザが文字情報を入力するために用いるもの入力デバイスである。なお、図示されていないが、ディスプレイ１０の画面上に表示されるマウスカーソルを操作するためのマウスも接続されている。

【００４１】

ＩＣカードリーダライタ１２はＩＣカード１５（スマートカードともいう）からの情報の読み出し、および情報の書き込みを行うためのデバイスである。このＩＣカード１５は例えばプラスチックのカード上に集積回路（ＩＣ）が設けられたものであり、この集積回路はＩＣカードリーダライタ１２と電気的に接続するための接点部と、各種処理を行う処理部と、情報を記録する記録部を備える。

【００４２】

本例でのＩＣカードリーダライタ１２とＩＣカード１５は物理的に接触して情報の読み出しおよび書きこみを行うものを説明するが、非接触型のＩＣカードリーダライタとＩＣカードもあり、そちらを利用することも可能である。

【００４３】

上記クライアント１と同様に、本発明の他のプログラムはこのＩＣカード１５の記録部に記録されており、ＩＣカード１５の処理部を制御して本発明の処理を行うよう動作する。

【００４４】

以下、本発明のプログラムで行われる処理について詳細に説明する。

【００４５】

まず、例として、ＬＯＧＯＮ画面を表示し、ＩＤとパスワードを入力させてユーザ認証を行うシステムでの処理について図３～図６を用いて説明する。ここでのＬＯＧＯＮ画面は、ＯＳの起動時やサーバによるサービスを提供する初期段階

などに表示されるものである。

【００４６】

図３および図４は、本実施の形態における認証処理を説明するのための処理フローチャートである。

【００４７】

また、図５および図６は上記認証処理での画面表示の遷移を示す図である。

【００４８】

まず、認証情報を入力するための画面表示であるＬＯＧＯＮ画面が表示されると（図５（ａ））、個人識別情報（以下、ＰＩＮと称する）を入力させるための画面を表示する。（ステップＳ１１，図５（ｂ））

このＰＩＮの入力画面の表示は、前記ＬＯＧＯＮ画面が表示されたことを検出してそれをトリガとして表示するように構成してもよいし、図示しない画面表示指示ボタンが操作されたことを検出して表示するように構成してもよい。

【００４９】

上記ＰＩＮの入力画面が表示された状態においてキャンセル指示がされると（ステップ１２）、本認証処理をキャンセルして終了する。一方、ＰＩＮ入力画面にユーザがキーボード１１を用いてＰＩＮを入力して入力完了指示を行うと、入力されたＰＩＮはＩＣカード１５に供給される。（ステップＳ１３）

ＩＣカード１５においては、クライアント本体から供給されるＰＩＮと記録部に記録されているＰＩＮとの照合を行う。（ステップＳ１４）

ステップＳ１４の照合の結果、ユーザによって入力されたＰＩＮが記録部に記録されているＰＩＮが一致しない場合、クライアント本体にその不一致の旨の情報を送信する。

【００５０】

クライアント本体はＩＣカード１５から前記不一致の旨の情報を受信すると、ユーザに入力されたＰＩＮが正しくないことをメッセージとして画面上に表示する。（ステップＳ１５，Ｓ１６）

また、ＩＣカード１５はユーザによって入力されたＰＩＮと記録部に記録されているＰＩＮが一致した場合には、クライアント本体にその一致の旨の情報を送

信し、その後のクライアント本体からのアクセスを許可する状態に設定する。

【００５１】

クライアント本体（ＣＰＵ４）はＩＣカード１５からＰＩＮが一致する旨の情報を受信すると、ＩＣカード１５に記録されているアプリケーション名の一覧を要求する。ＩＣカード１５はその要求を受信して、記録部に記録されている各レコードの情報からアプリケーション名に関する情報を読み出し、クライアント本体に供給する。

【００５２】

クライアント本体はＩＣカード１５からアプリケーション名に関する情報を受信し、それを選択候補として画面上に表示する。（ステップＳ１７，図６（ｃ））

ユーザは現在のシステム（アプリケーション）に応じたアプリケーション名を選択し、選択確定操作を行う。（ステップＳ１８）

ユーザによってアプリケーション名が選択されると、選択されたアプリケーション名に関する情報をＩＣカード１５に供給し、該選択アプリケーションに対応する認証情報の読み出しを要求する。このとき、画面上に表示していた選択候補の一覧は消去する。

【００５３】

ＩＣカード１５はアプリケーション名に関する情報とそれに対応する認証情報の読み出し要求を受信し、供給されるアプリケーション名に関する情報に基づき記録部の各レコードから要求に合致する情報を読み出してクライアント本体に供給する。

【００５４】

クライアント本体はＩＣカード１５から供給された認証情報を受信し、その認証情報をＬＯＧＯＮ画面の所定の入力フィールドに設定する。（図６（ｄ））

入力フィールドに認証情報が設定されると、ユーザは確定操作を行う。

【００５５】

認証情報が確定されると、その認証情報がシステムに供給され認証処理（照合処理）が行われる。（ステップＳ１９）

ステップＳ１９による認証処理の結果、入力された認証情報と一致する情報があればＬＯＧＯＮ処理を行う。（ステップＳ２０）

また、入力された認証情報に一致する情報がなければ、ステップＳ１７で表示したアプリケーション名の一覧を画面上に表示して、再び上記ステップＳ１８～Ｓ２０の処理を行う。

【００５６】

以上のように、ユーザがＰＩＮを入力し、ＩＣカード１５から読み出され画面上に表示されるアプリケーション名一覧の中から所望のものを選択するだけで、該アプリケーションに関する認証情報を入力フィールドに設定することが可能になる。

【００５７】

従って、ユーザは１つの識別情報を覚えておくだけで、複数のシステムを利用することが可能となる。また、ＩＣカードの記録部に記録されている情報はそのＩＣカードの処理部のみが読み出し可能なため、他人による認証情報への直接アクセスすることによる盗聴を防止することが可能となる。

【００５８】

上記例では認証情報を入力させるログイン画面を表示するシステム（アプリケーション）について説明しているが、これに限定されるものでなく、画面焼き付き防止のためのスクリーンセーバからの復帰時に表示されるパスワード入力画面にも本発明は適用することができる。すなわち、利用者ＩＤやパスワードを入力する状態になるものに関して本発明は応用することが可能である。

【００５９】

また、上記例ではユーザがアプリケーション名の一覧から所望のものを選択する構成をとっているが、現アプリケーション（システム）の識別情報が取得できる場合、ＩＣカード１５からアクセス許可を受信した後、該識別情報を基にＩＣカード１５に該アプリケーションの認証情報を要求するように構成してもよい。これにより、アプリケーション名の一覧を画面表示させ、ユーザに選択させるという操作を削減することができる。

【００６０】

次に、認証処理に使用される認証情報を変更する際に、システム（以下、アプリケーションともいう）が管理している認証情報とＩＣカードに記録された認証情報の同期をとる処理を説明する。

【００６１】

図７および図８は、本実施の形態における認証情報の変更処理を説明するのための処理フローチャートである。

【００６２】

また、図９は上記変更処理での画面表示例を示す図である。

【００６３】

まず、パスワードを変更するための入力画面が表示されると、個人識別情報（ＰＩＮ）を入力させるための画面を表示する。（ステップＳ２１）

このＰＩＮの入力画面の表示は、システムで用意している既存のパスワード変更入力画面が表示されたことを検出してそれをトリガとして表示するように構成してもよいし、専用のパスワード変更入力画面を表示するように構成してもよい。

【００６４】

上記ＰＩＮの入力画面が表示された状態においてキャンセル指示がされると（ステップ２２）、本変更処理をキャンセルして終了する。一方、ＰＩＮ入力画面にユーザがキーボード１１を用いてＰＩＮを入力して入力完了指示を行うと、入力されたＰＩＮはＩＣカード１５に供給される。（ステップＳ２３）

ＩＣカード１５においては、クライアント本体から供給されるＰＩＮと記録部に記録されているＰＩＮとの照合を行う。（ステップＳ２４）

ステップＳ２４の照合の結果、ユーザによって入力されたＰＩＮが記録部に記録されているＰＩＮが一致しない場合（ステップＳ２５）、クライアント本体にその不一致の旨の情報を送信する。

【００６５】

クライアント本体はＩＣカード１５から前記不一致の旨の情報を受信すると、ユーザに入力されたＰＩＮが正しくないことをメッセージとして画面上に表示する。（ステップＳ２６）

また、ＩＣカード１５はユーザによって入力されたＰＩＮと記録部に記録されているＰＩＮが一致した場合には、クライアント本体にその一致の旨の情報を送信し、その後のクライアント本体からのアクセスを許可する状態に設定する。

【００６６】

クライアント本体（ＣＰＵ４）はＩＣカード１５からＰＩＮが一致する旨の情報を受信すると、図９のパスワードの入力フィールドへの情報入力を有効にする。

【００６７】

ユーザは有効になったパスワードの入力フィールドへ古いパスワード、新しいパスワード、確認のための新しいパスワードをそれぞれ入力し、入力確定操作を行う。

【００６８】

パスワード変更のための入力情報が確定されると、システムがパスワードの変更処理を行うと共に、クライアント本体（ＣＰＵ４）はＩＣカード１５に対し、ＩＣカード１５に記録されているアプリケーション名の一覧を要求する。ＩＣカード１５はその要求を受信して、記録部に記録されている各レコードの情報からアプリケーション名に関する情報を読み出し、クライアント本体に供給する。

【００６９】

クライアント本体はＩＣカード１５からアプリケーション名に関する情報を受信し、それを選択候補として画面上に表示する。（ステップＳ２７）

ユーザは現在のシステム（アプリケーション）に応じたアプリケーション名を選択し、選択確定操作を行う。（ステップＳ２８）

ユーザによってアプリケーション名が選択されると、選択されたアプリケーション名に関する情報と共に、変更要求としてユーザによって入力されたパスワードに関する各情報をＩＣカード１５に供給する。このとき、画面上に表示していた選択候補の一覧は消去する。

【００７０】

ＩＣカード１５は新たなパスワードへの変更要求を受信し、供給されるアプリケーション名に関する情報とパスワードに関する情報に基づき記録部の各レコー

ドから該アプリケーション名に合致するパスワードの情報フィールドを新たなパスワードに書き換える。（ステップＳ２９）

また、選択されたアプリケーションに関する情報のパスワードとユーザによって入力された古いパスワードが一致しないなど、現在のシステムに合致しない入力がされた場合には（ステップＳ３０）、ステップＳ２７で表示したアプリケーション名の一覧を画面上に表示して、再び上記ステップＳ２８～Ｓ３０の処理を行う。

【００７１】

このような処理によって、システムおよびＩＣカード１５内のパスワードを一度の入力で変更することができる。従って、ユーザによるパスワード変更入力の手間を省くことが可能となる。

【００７２】

次に、ＩＣカード１５に複数の証明書を記録させて利用する例について説明する。

【００７３】

この証明書は秘密鍵と呼ばれ、例えばＷＷＷサーバのデータ暗号化で使用され、セキュリティで保護されたページの閲覧などにおいて必要になるものである。

【００７４】

図１０および図１１はＷＷＷブラウザによりセキュリティで保護されたページの閲覧時に証明書を使用するときの処理フローチャートである。

【００７５】

また、図１２および図１３はそのＷｅｂサイト閲覧時の画面表示の遷移を示す図である。

【００７６】

まず、ＷＷＷブラウザでセキュリティで保護されたページのＵＲＬを直接入力する、またはリンクを指定すると、ブラウザは証明書の入力を要求する。（図１２（ａ））

この要求があると、ユーザはＩＣカード１５をＩＣカードリーダライタ１２にセットする。

【００７７】

ＩＣカード１５がセットされると、個人識別情報（ＰＩＮ）を入力させるための画面を表示する。（ステップＳ３１，図１２（ｂ））

上記ＰＩＮの入力画面が表示された状態においてキャンセル指示がされると（ステップ３２）、本認証処理をキャンセルして終了する。一方、ＰＩＮ入力画面にユーザがキーボード１１を用いてＰＩＮを入力して入力完了指示を行うと、入力されたＰＩＮはＩＣカード１５に供給される。（ステップＳ３３）

ＩＣカード１５においては、クライアント本体から供給されるＰＩＮと記録部に記録されているＰＩＮとの照合を行う。（ステップＳ３４）

ステップＳ３４の照合の結果、ユーザによって入力されたＰＩＮが記録部に記録されているＰＩＮが一致しない場合、クライアント本体にその不一致の旨の情報を送信する。

【００７８】

クライアント本体はＩＣカード１５から前記不一致の旨の情報を受信すると、ユーザに入力されたＰＩＮが正しくないことをメッセージとして画面上に表示する。（ステップＳ３５，Ｓ３６）

また、ＩＣカード１５はユーザによって入力されたＰＩＮと記録部に記録されているＰＩＮが一致した場合には、クライアント本体にその一致の旨の情報を送信し、その後のクライアント本体からのアクセスを許可する状態に設定する。

【００７９】

クライアント本体（ＣＰＵ４）はＩＣカード１５からＰＩＮが一致する旨の情報を受信すると、ＩＣカード１５に記録されている証明書名の一覧を要求する。ＩＣカード１５はその要求を受信して、記録部に記録されている各証明書名に関する情報を読み出し、クライアント本体に供給する。

【００８０】

クライアント本体はＩＣカード１５から証明書名に関する情報を受信し、それを選択候補として画面上に表示する。（ステップＳ３７，図１３（ｃ））

ユーザは現在のページに応じた証明書名を選択し、選択確定操作を行う。（ステップＳ３８）

ユーザによって証明書名が選択されると、選択された証明書名に関する情報をＩＣカード１５に供給し、選択された証明書名に対応するデータの読み出しを要求する。このとき、画面上に表示していた選択候補の一覧は消去する。

【００８１】

ＩＣカード１５は証明書名に関する情報とそれに対応するデータの読み出し要求を受信し、供給される証明書名に関する情報に基づき記録部の各レコードから要求に合致する情報を読み出してクライアント本体に供給する。

【００８２】

クライアント本体はＩＣカード１５から供給された証明書のデータを受信し、その証明書のデータを用いて認証処理を行う。（ステップＳ３９）

ステップＳ３９による認証処理の結果、正しければセキュリティで保護されたページの表示を行う。（ステップＳ４０）

また、証明書のデータが正しくなければ、ステップＳ３７で表示した証明書名の一覧を画面上に表示して、再び上記ステップＳ３８～Ｓ４０の処理を行う。

【００８３】

このように、クライアント本体に証明書のデータを持つのではなく、ＩＣカードのような可搬型の記録媒体に記録しておき、必要に応じてそれから読み出し利用する形態をとることにより、クライアント本体を他人が利用してもこの証明書のデータを記録した記録媒体がなければ、セキュリティで保護されたページの閲覧はできなくなる。

【００８４】

よって、高度なセキュリティを実現することが可能となる。

【００８５】

最後に、ＩＣカード１５の記録部に記録されるデータの構造について説明する。

【００８６】

図１４は、ＩＣカードの記録部に記録されるデータの構造を示す図である。

【００８７】

１レコードは、アプリケーションＩＤ、ユーザＩＤ、パスワード、ドメイン、

拡張の各フィールドからなる。

【００８８】

そして、ＩＣカード１５の記録部には複数のアプリケーション（システム）のためにそれぞれ対応する複数のレコードが記録されている。

【００８９】

アプリケーションＩＤのフィールドは、アプリケーションを特定するための情報が記録されるものである。これを用いてクライアント本体での選択候補一覧が作成され、また、認証情報を読み出す際のキーとなるものである。

【００９０】

ユーザＩＤのフィールドは、対応するアプリケーションのユーザＩＤが記録されるものである。

【００９１】

パスワードのフィールドは、対応するアプリケーションのユーザＩＤと対をなすパスワードが記録されるものである。

【００９２】

ドメインのフィールドは、上記処理の説明では用いられていないが、サーバにログインする際に用いられる情報が記録されるものである。

【００９３】

拡張のフィールドは、拡張情報が次のレコードに続くか否かを示すための情報が記録されるものである。

【００９４】

以上、本発明の実施の形態を説明した。

【００９５】

なお、本発明は以下の特徴も有する。

（発明１）

利用者により入力される入力識別情報と記録媒体に記録されている固有の識別情報との照合を制御する制御部であって、該制御部は前記入力識別情報を前記記録媒体に供給する供給部と、

前記記録媒体の照合部による前記入力識別情報と前記固有識別情報との照合結果

を受信する受信部とを備え、

前記照合結果に応じて、前記記録媒体に記録されている複数のシステムにそれぞれ対応する認証情報のうち読み出される対象システムに関する認証情報を認証処理の入力情報として設定する設定部と、

を備える認証制御装置。

（発明２）

上記発明１において、前記照合結果が一致の場合に、前記複数のシステムを選択候補として表示させる表示制御部と、

前記選択候補から対象システムを選択する選択部とを備え、

前記設定部は前記選択された対象システムに関する認証情報を認証処理の入力情報として設定する認証制御装置。

（発明３）

上記発明２において、前記記録媒体に情報の読み出し要求を行う要求部を備え、

前記表示制御部は、前記要求により読み出される前記記録媒体に記録された複数のシステムに関する情報を選択候補として表示させる認証制御装置。

（発明４）

コンピュータに、

利用者により入力される入力識別情報と記録媒体に記録されている固有の識別情報との照合を制御する手順と、

前記照合結果に応じて、前記記録媒体に記録されている複数のシステムにそれぞれ対応する認証情報のうち読み出される対象システムに関する認証情報を認証処理の入力情報として設定する手順とを実行させるプログラムであり、さらに前記制御する手順は、

前記入力識別情報を前記記録媒体に供給する手順と、

前記記録媒体の照合部による前記入力識別情報と前記固有識別情報との照合結果を受信する手順と

からなるプログラムを記録したコンピュータ読み取り可能な記録媒体。

（発明５）

発明４において、前記照合結果が一致の場合に、前記複数のシステムを選択候補として表示する手順と、

前記選択候補から対象システムを選択する手順と、

前記記録媒体から読み出される前記選択された対象システムに関する認証情報を認証処理の入力情報として設定する手順と、

をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【００９６】

これら発明の構成により、ユーザは１つの識別情報を記憶しおくだけで複数のシステムのそれぞれに対応する認証情報を覚えておく必要がなくなる。さらに、識別情報の照合は記録媒体が行い、本装置は照合の要求と照合結果の受信を行う構成であるため、本装置が記録媒体に直接読み出しにいくことを避けることができ、記録媒体に記録されている認証情報のセキュリティが向上する。

【００９７】

また、本発明のプログラムも上記処理をコンピュータに実行させることで、同様の作用効果を得ることができる。

【００９８】

【発明の効果】

以上のように、本発明によって、ユーザは１つの識別情報を覚えておくだけで、複数のシステムを利用することができ、他人による認証情報への直接アクセスすることによる盗聴を防止することが可能となる。

【００９９】

また、一度の入力で複数の記録部に記録された認証情報を変更することができるため、ユーザによる認証情報の変更操作の手間を省くことが可能となる。

【０１００】

さらに、高度なセキュリティを実現することが可能となる。

【図面の簡単な説明】

【図１】

本発明のシステム構成図である。

【図２】

コンピュータの概略構成を示す図である。

【図３】

本実施の形態における認証処理を説明するのための処理フローチャート（その１）である。

【図４】

本実施の形態における認証処理を説明するのための処理フローチャート（その２）である。

【図５】

認証処理での画面表示の遷移を示す図（その１）である。

【図６】

認証処理での画面表示の遷移を示す図（その２）である。

【図７】

本実施の形態における認証情報の変更処理を説明するのための処理フローチャート（その１）である。

【図８】

本実施の形態における認証情報の変更処理を説明するのための処理フローチャート（その２）である。

【図９】

認証情報の変更処理での画面表示例を示す図である。

【図１０】

セキュリティで保護されたページの閲覧時に証明書を使用するときの処理フローチャート（その１）である。

【図１１】

セキュリティで保護されたページの閲覧時に証明書を使用するときの処理フローチャート（その２）である。

【図１２】

Ｗｅｂサイト閲覧時の画面表示の遷移を示す図（その１）である。

【図１３】

Ｗｅｂサイト閲覧時の画面表示の遷移を示す図（その２）である。

【図１４】

ＩＣカードの記録部に記録されるデータの構造を示す図である。

【符号の説明】

１　クライアント

２　サーバ

３　ネットワーク

４　ＣＰＵ

５　ＲＡＭ

６　ＨＤＤ（ハードディスクドライブ）

７　ＣＤ－ＲＯＭドライブ

８　ＦＤＤ（フロッピィディスクドライブ）

９　ＮＣＵ（ネットワーク制御ユニット）

１０　ディスプレイ

１１　キーボード

１２　ＩＣカードリーダライタ１２

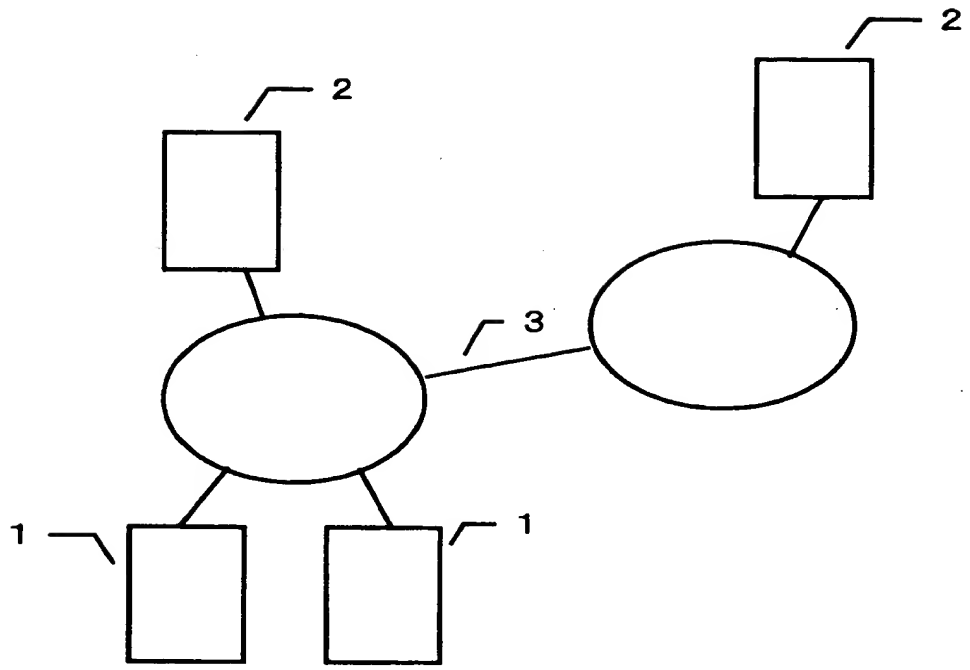
１３　ＣＤ－ＲＯＭ

１４　フロッピィディスク

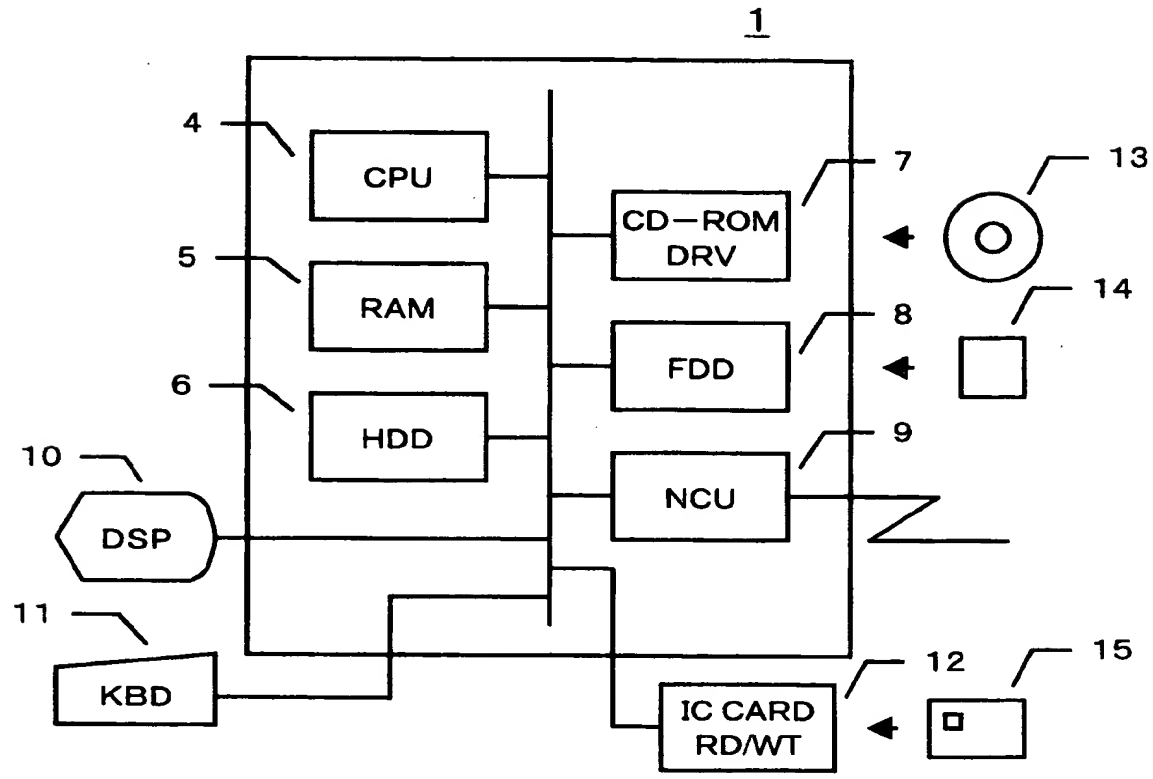
１５　ＩＣカード（スマートカード）

【書類名】　　図面

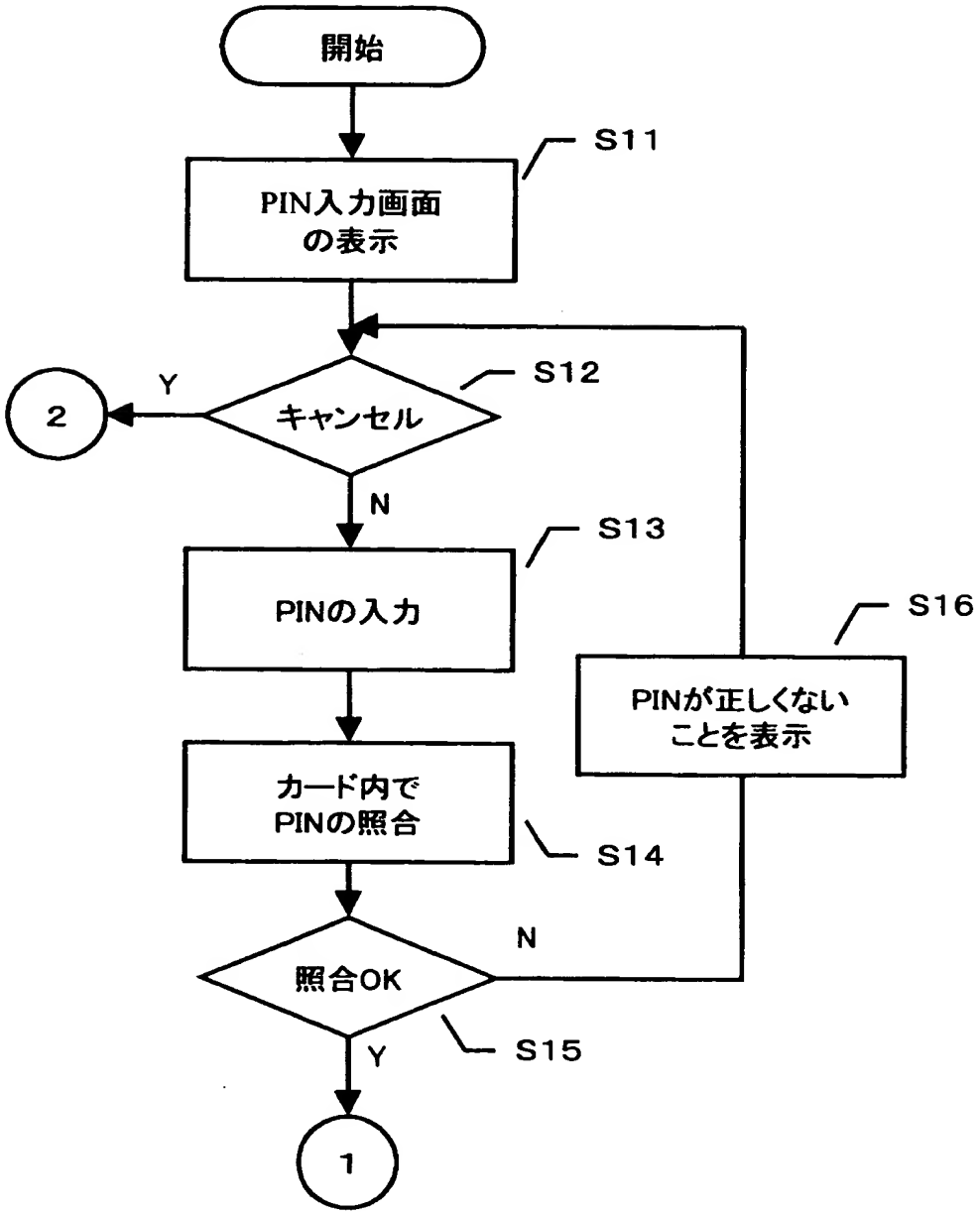
【図１】


2
2
3
1
1

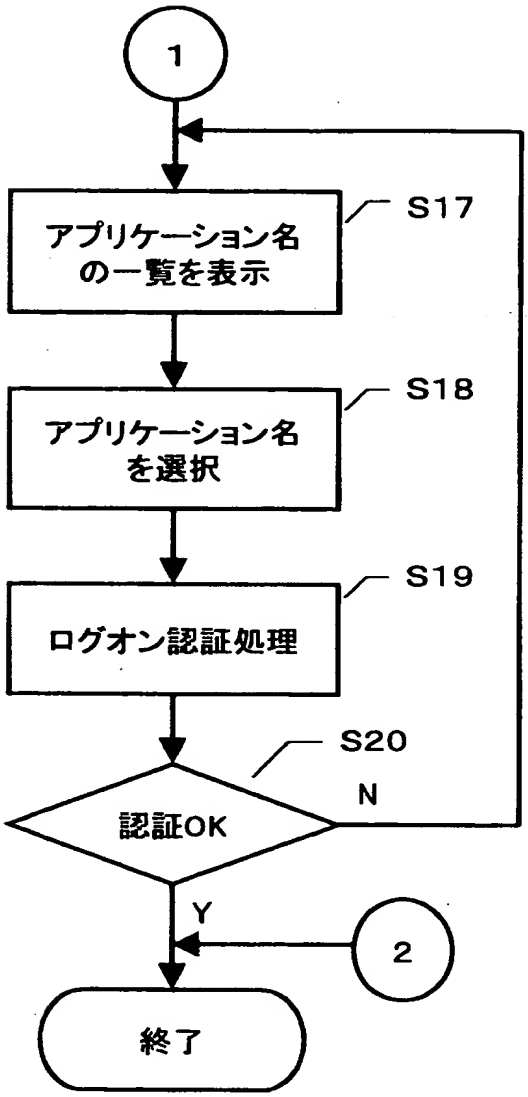
【図２】


1
4
CPU
5
RAM
6
HDD
10
DSP
11
KBD
7
CD−ROM
DRV
8
FDD
9
NCU
12
IC CARD
RD/WT
13
14
15

【図３】

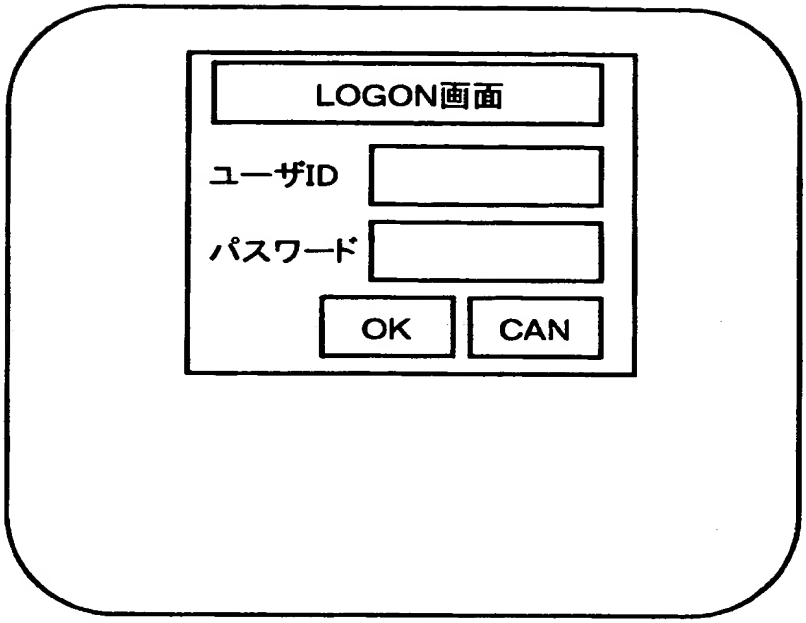

開始
S11
PIN入力画面
の表示
S12
Y
2
キャンセル
N
S13
PINの入力
S16
PINが正しくない
ことを表示
カード内で
PINの照合
S14
N
照合OK
S15
Y
1

【図４】

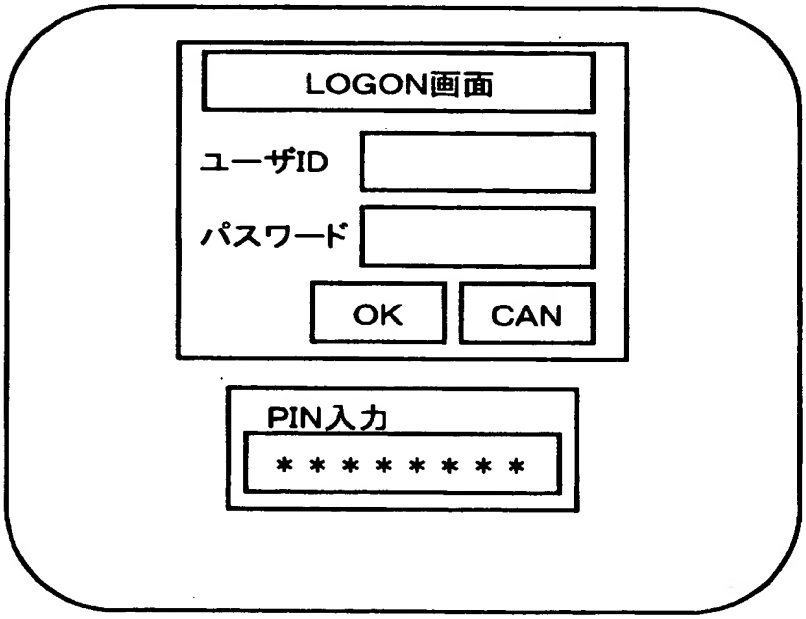

1
アプリケーション名の一覧を表示
S17
アプリケーション名を選択
S18
ログオン認証処理
S19
S20
認証OK
N
Y
2
終了

【図５】

(a)

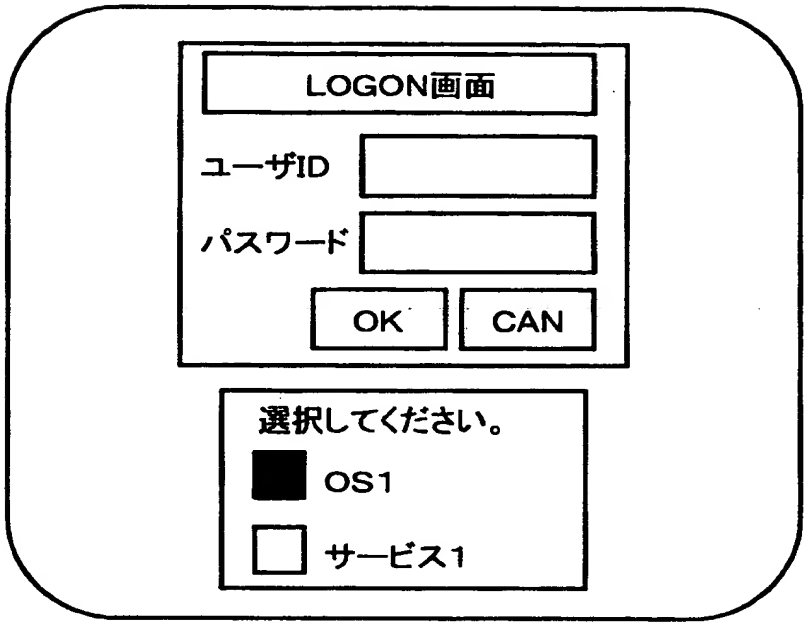


(b)

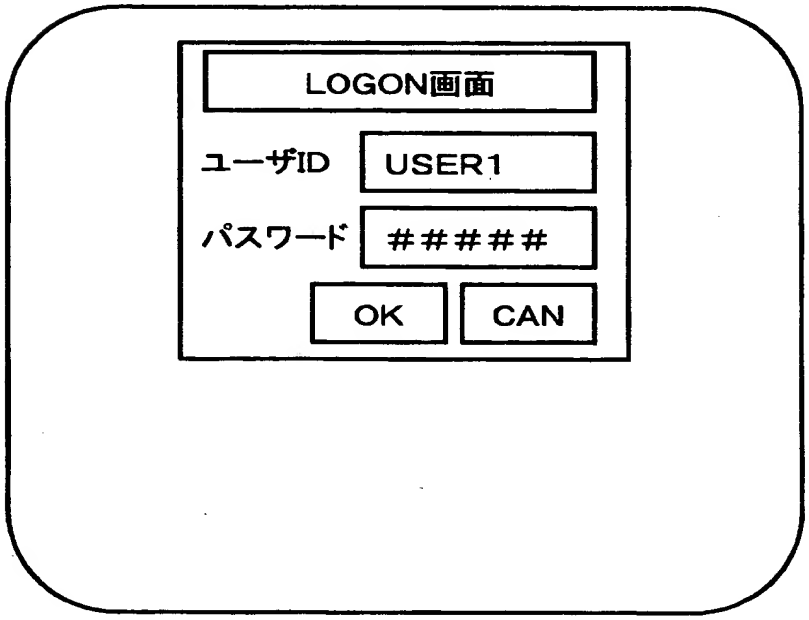


【図６】

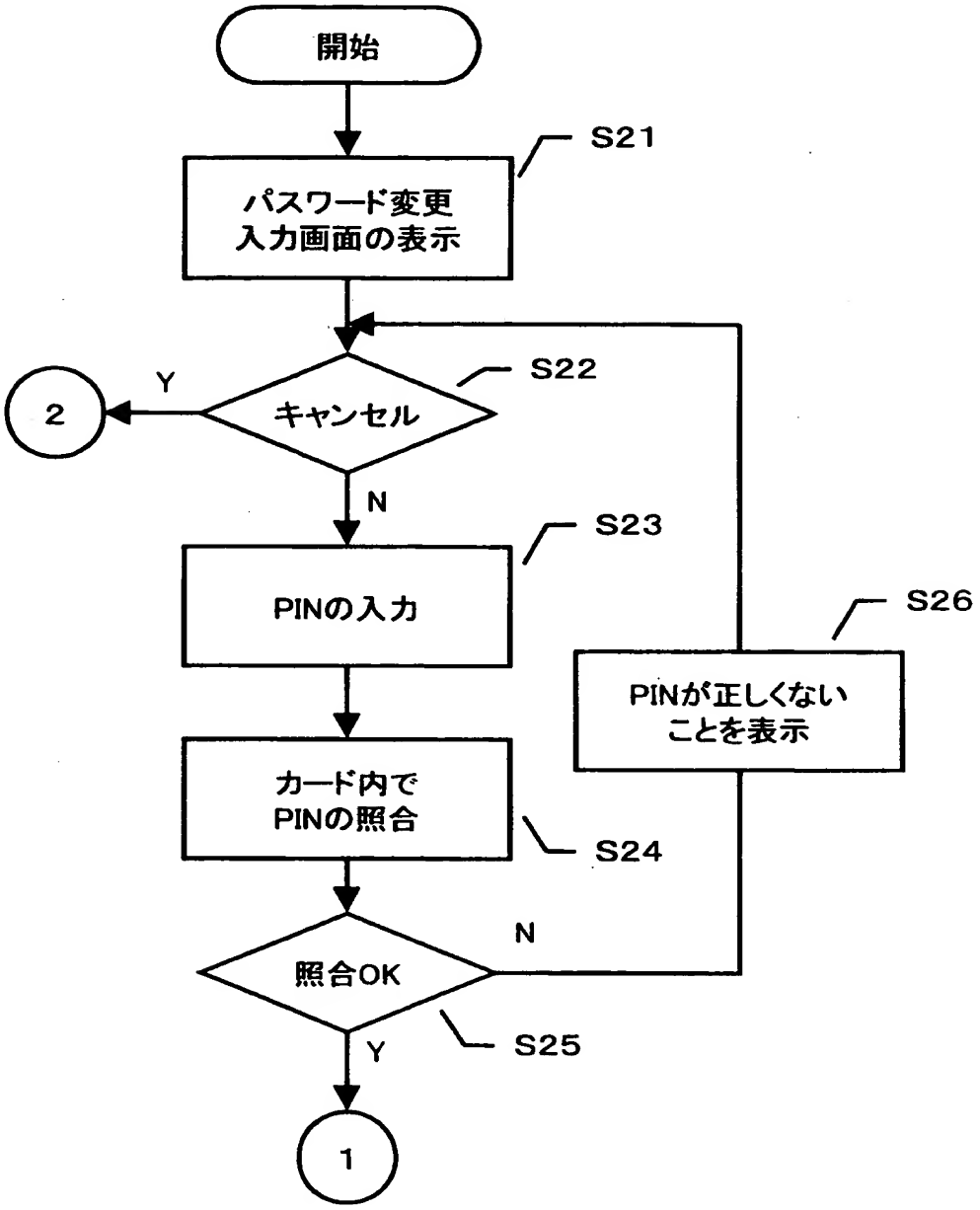
(c)


LOGON画面
ユーザID
パスワード
OK
CAN
選択してください。
OS1
サービス1

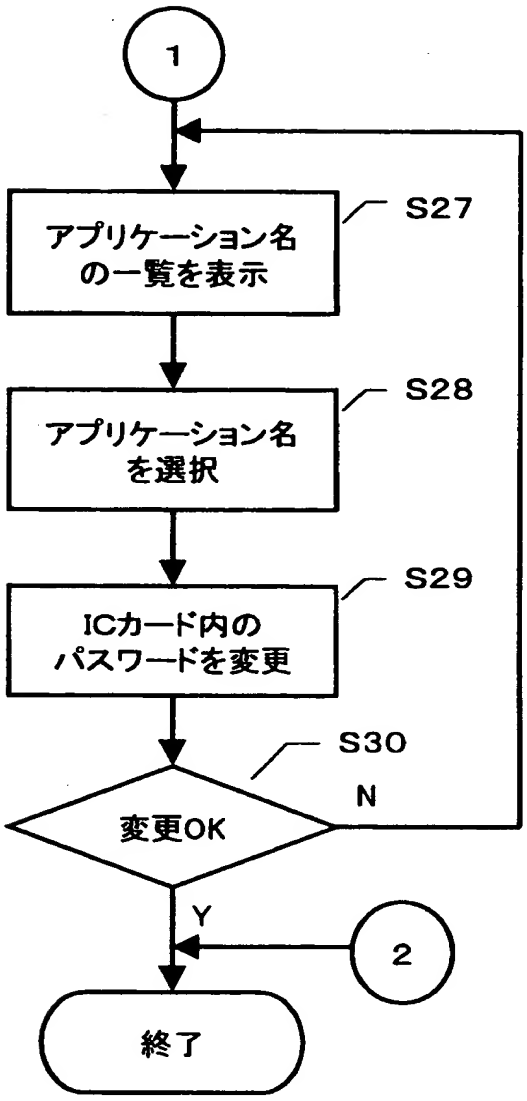
(d)


LOGON画面
ユーザID
USER1
パスワード
#####
OK
CAN

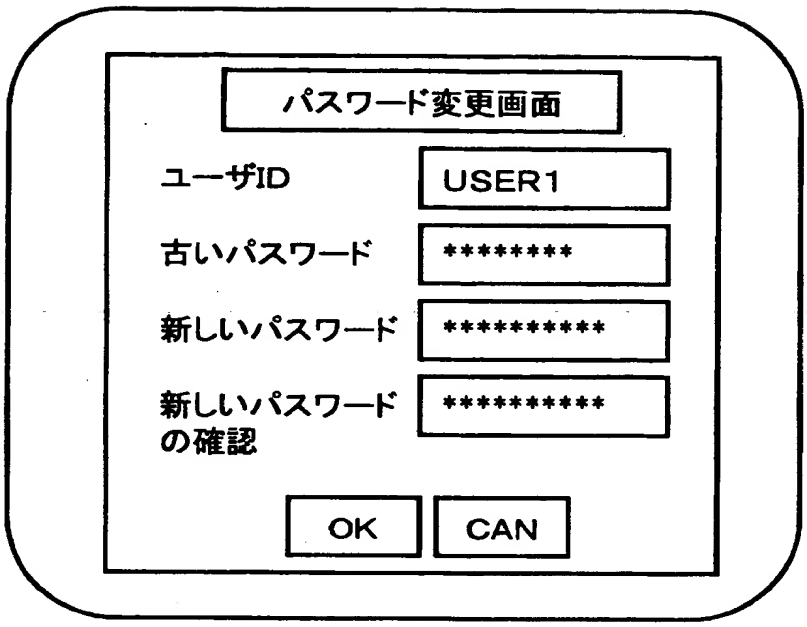
【図７】


開始
S21
パスワード変更
入力画面の表示
S22
Y
2
キャンセル
N
S23
PINの入力
S24
カード内で
PINの照合
N
照合OK
S25
Y
1
S26
PINが正しくない
ことを表示

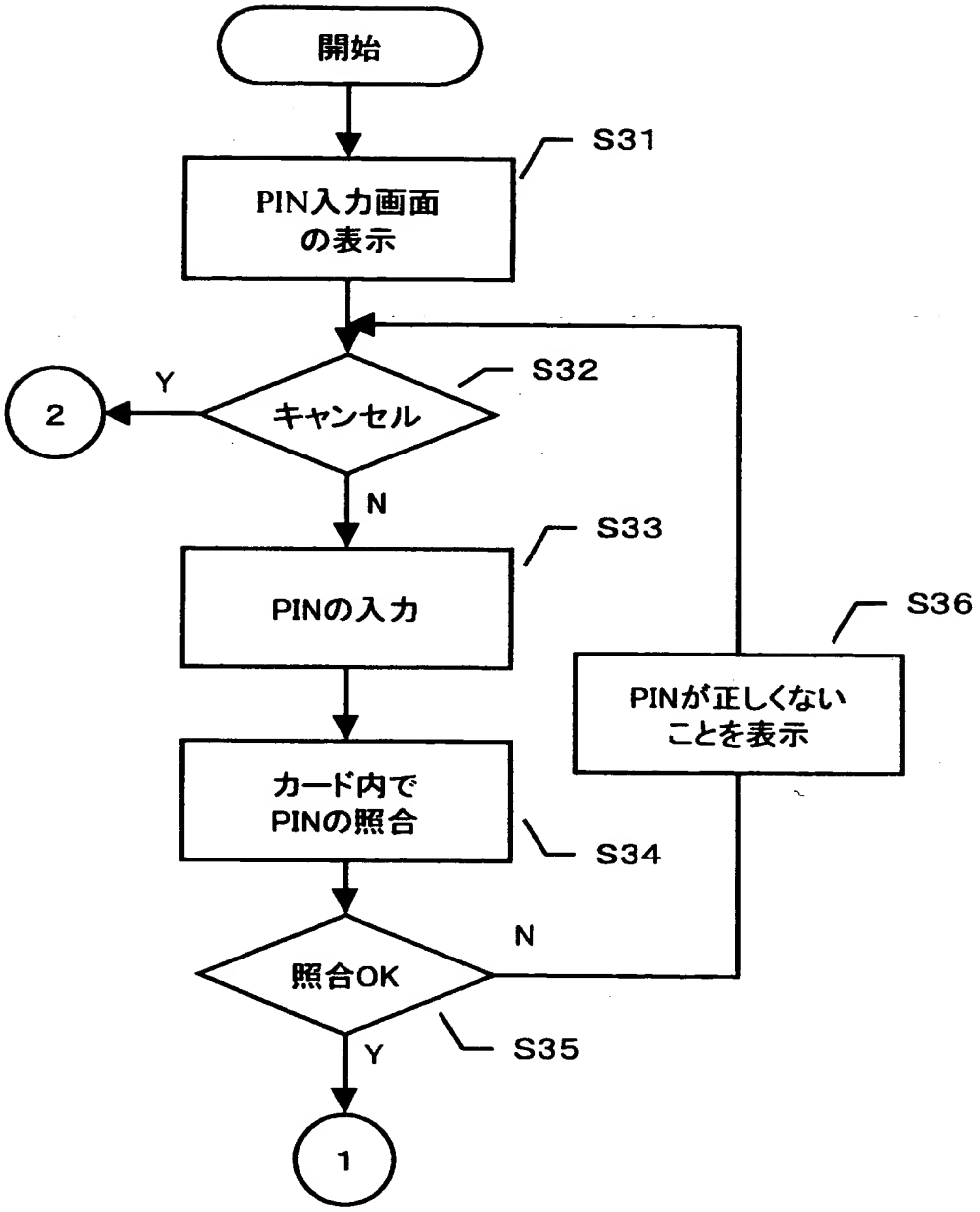
【図８】


1
アプリケーション名の一覧を表示
S27
アプリケーション名を選択
S28
ICカード内のパスワードを変更
S29
S30
変更OK
N
Y
2
終了

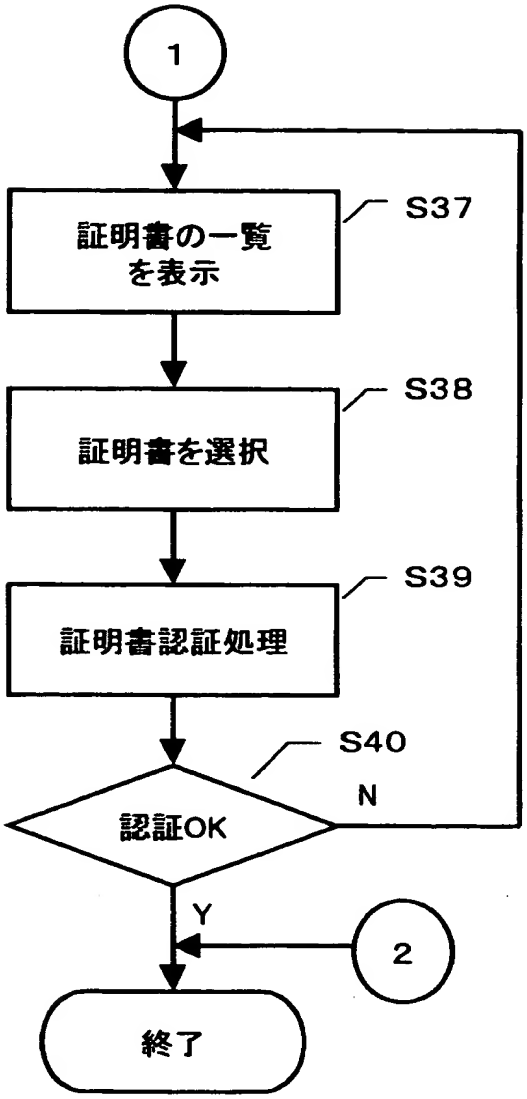
【図９】


パスワード変更画面
ユーザID
USER1
古いパスワード
****
新しいパスワード
****
新しいパスワードの確認
****
OK
CAN

【図１０】

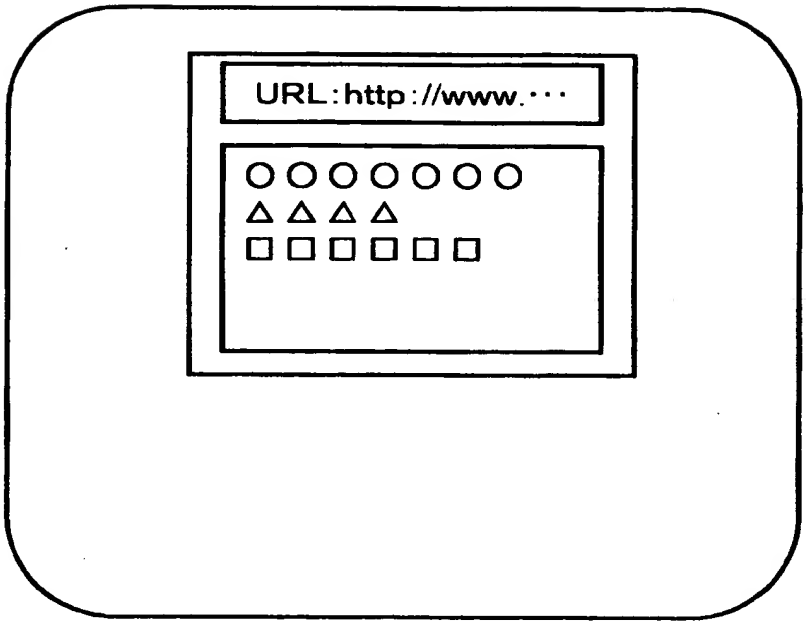

開始
S31
PIN入力画面
の表示
S32
Y
2
キャンセル
N
S33
PINの入力
S36
PINが正しくない
ことを表示
カード内で
PINの照合
S34
N
照合OK
S35
Y
1

【図１１】

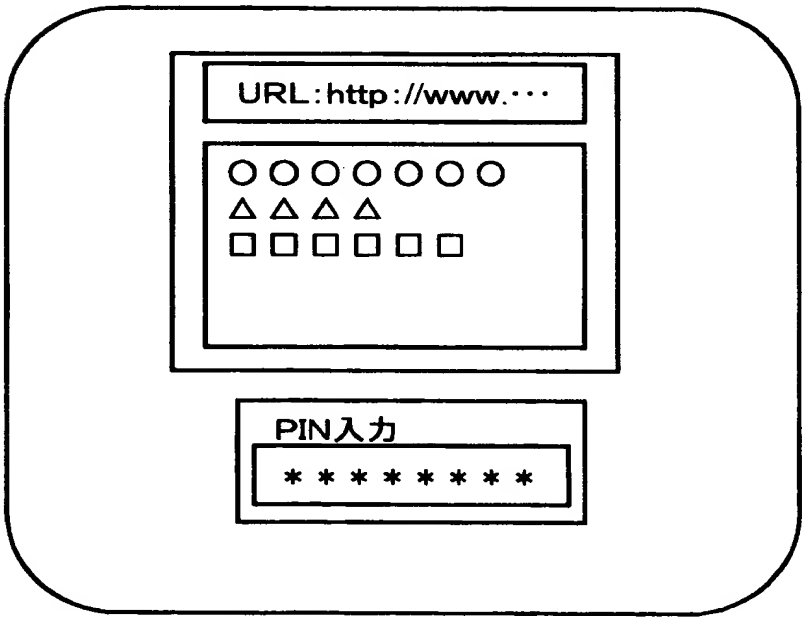


【図１２】

(a)

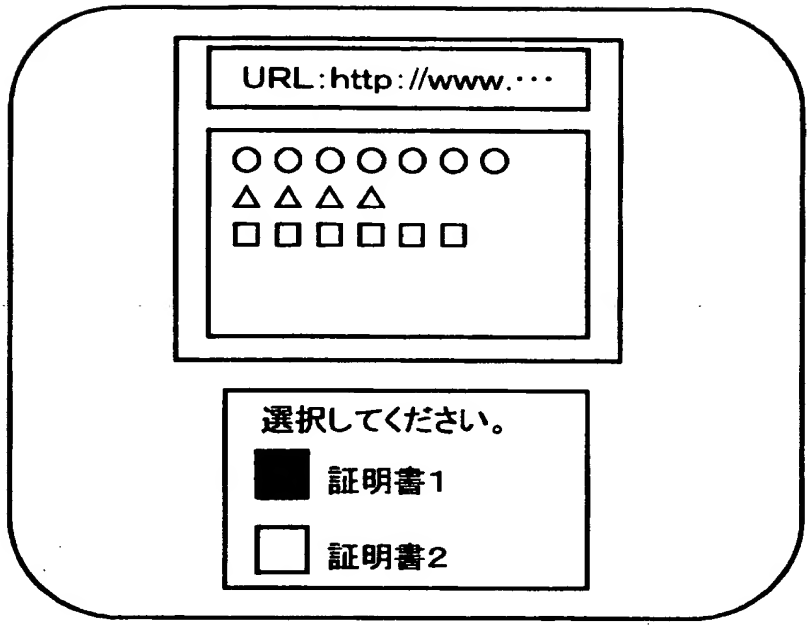


(b)

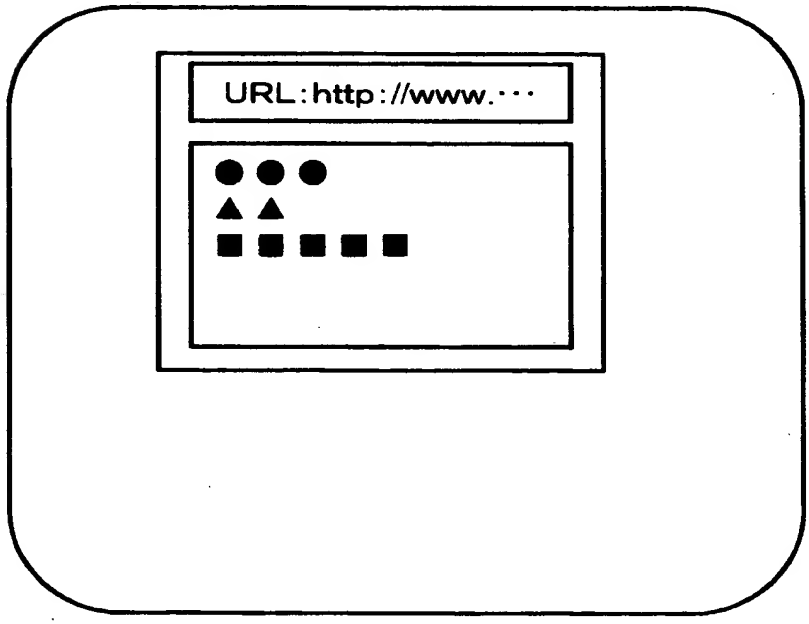


【図１３】

(c)



(d)



【図１４】

アプリケーションID	ユーザID	パスワード	ドメイン	拡張

【書類名】　　要約書

【要約】

【課題】　本発明は、複数のシステムに対する利用者の操作の簡易化、複数のシステムを利用する環境におけるセキュリティ向上のための認証制御装置、認証制御システム、記録媒体を提供する。

【解決手段】　利用者により入力される入力識別情報と記録媒体に記録されている固有の識別情報とを照合し、前記照合結果に応じて、前記記録媒体に記録されている複数のシステムにそれぞれ対応する認証情報のうち対象システムに関する認証情報を読み出し、前記読み出された認証情報を認証処理の入力情報として設定する。

【選択図】　図３

出　願　人　履　歴　情　報

識別番号　　〔０００００５２２３〕

１．変更年月日　　１９９６年　３月２６日
［変更理由］　住所変更
住　所　　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　　富士通株式会社